



Лекция №1

ВВЕДЕНИЕ В КУРС

Дисциплина: Криптографическая защита информации

Преподаватель: Миронов Константин Валерьевич

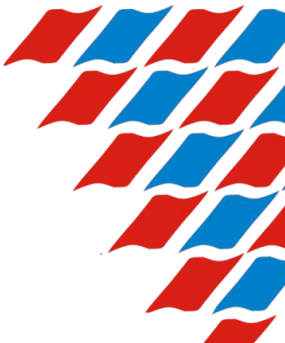
Поток: БПС-3

Учебный год: 2020/21



Содержание лекции

- **Структура курса**
- Общие сведения о криптографии
- Исторический обзор

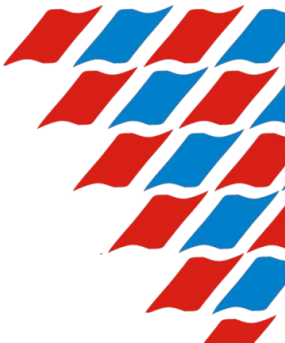


Структура Курса

9 лекций

- Дистанционное проведение:
 - Объявление в СДО
 - Лекция в Zoom по расписанию
 - Презентация на СДО
 - Возможно: видео лекции на youtube
- Содержание:
 - Теоретический материал
 - Устные опросы
 - Доклады по материалу СРС

**Посещение занятий не является
обязательным и само по себе на зачет не
влияет**

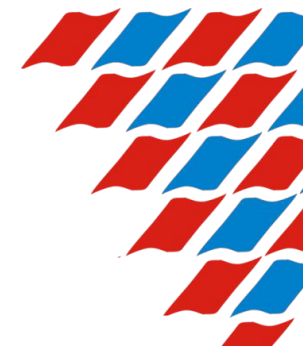


Структура Курса

9 лекций

Пожелания к докладам:

- Презентация 7-10 слайдов
- Выступление 7-10 минут
- Для каждого алгоритма рассмотреть:
 - общие характеристики и особенности,
 - краткую предысторию разработки,
 - процесс зашифровки и расшифровки (вычисления хеш-функций, постановки и проверки электронной подписи),
 - история криптоанализа и найденные уязвимости,
 - сведения о реальном применении.
- Файл презентации должен быть выложен на форуме СДО



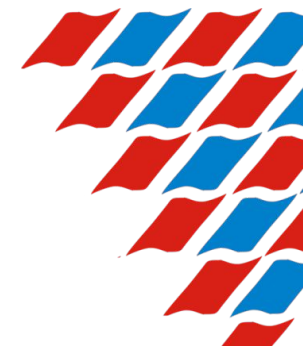
Структура Курса

3 лабораторные работы

- Каждая подгруппа разбивается на 4 бригады
 - Список бригад фиксированный, сдается преподавателю для настройки бригад на СДО
- Лабораторные работы №1 и 2
 - Выполняются самостоятельно, побригадно
 - Шифруемый текст должен содержать фамилии студентов
 - Отчет от имени бригады грузит на СДО любой студент бригады
- Лабораторная работа №3
 - Выполняется в чатах СДО в реальном времени

3 практики

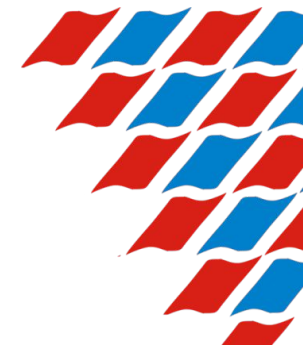
- Список задач публикуется на СДО заранее
- По расписанию в Zoom студент описывает решение задач



Структура Курса

зачет

- Лабораторные работы должны быть сданы
- По итогам активности на лекциях и практиках возможен автомат
 - Ответы при устных опросах по теоретическому материалу – необходимое условие, чтобы можно было делать доклады на лекциях и решать задачи на практиках
- 1-я часть зачета: 1 устный теоретический вопрос на знание базовых понятий
- 2-я часть зачета: 2 задачи письменно (допустимо пользоваться лекциями)
 - 1 задача: расчеты и здравый смысл
 - 1 задача: построение блок-схемы/псевдокода по словесному описанию
 - Задачи аналогичны решаемым на практиках
- Обе части надо сдать в один день, иначе 1-я не засчитывается

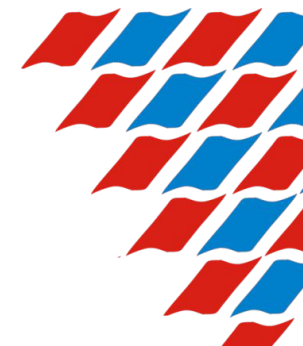


Структура Курса

Основные темы

- Симметричное шифрование – базовые операции, режимы шифрования, блочные и поточные алгоритмы, генераторы (псевдо)случайных последовательностей
- Хэш-функции, коды аутентификации сообщений, функции формирования ключа
- Парольная защита – хеширование паролей, радужные таблицы, криптографическая соль
- Асимметричная криптография – шифрование с открытым ключом, электронная подпись распределение ключей, инфраструктуры открытых ключей
- Модные и перспективные направления - системы распределенного реестра, квантовые и постквантовые алгоритмы, гомоморфное шифрование и т.п.

Криптография эллиптических кривых и стеганография изучаются в рамках курсов «Программно-аппаратная защита информации» и «Теория информационной безопасности»



Структура Курса

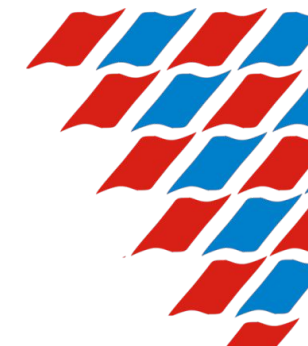
Рассматриваемые алгоритмы

- Блочные симметричные шифры – **3DES, AES, RC2, RC5, RC6, Blowfish, Twofish, Threefish, Магма, Кузнечик**
- Режимы шифрования – **ECB, CBC, PCBC, CFB, OFB, CTR, XTS, RandomDelta, OCB**
- Поточные шифры – **A3, RC4, Salsa20**
- Хэш-функции – на базе функции сжатия (**SHA-2, MD6, Blake, ГОСТ Р 34.11-94, Стрибог**), на базе криптографической губки (**SHA-3, Luffa**), имитовставки (**CBC-MAC, HMAC, UMAC**), функции формирования ключа (**PBKDF2, scrypt, Argon2**)
- Асимметричные универсальные – **RSA, алгоритм Эль-Гамала, алгоритм Рабина, ECC**
- Электронная подпись – **DSA/DSS, алгоритм Лэмпорта, алгоритм Винтерница, ГОСТ Р 34.10-2012**

Алгоритмы, рассматриваемые на лекциях

Алгоритмы, изучаемые в рамках СРС и представляемые студентами в докладах

Алгоритмы, изучаемые в рамках курса «Программно-аппаратная защита информации»



Содержание лекции

- Структура курса
- **Общие сведения о криптографии**
 - **Основные понятия**
 - **Симметричная и асимметричная криптография**
 - **Хэш-функции**
 - **Стеганография**
 - **Криптоанализ и правило Керкгоффса**
- Исторический обзор

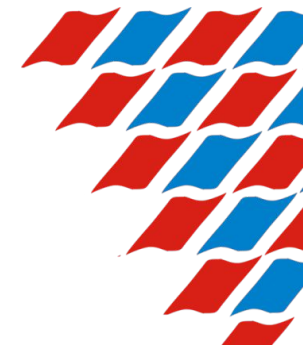


Общие сведения

- Криптографическая ЗИ – ЗИ путем ее модификации
- **Криптография** - инженерно-техническая дисциплина; занимается математическими методами защиты информации
- **Криптология** - отрасль дискретной математики; рассматривает математические модели криптографических схем.
- **Криптосинтез** – построение криптографических алгоритмов
- **Криптоанализ** – исследование методов взлома алгоритма

Альтернативный вариант – вместо криптографии термин криптология, вместо криптосинтеза – термин криптография

Определения в курсе не везде математически строги и не всегда точно соответствуют имеющимся в литературе/интернете. Во-первых, математически строгие определения, например, в теории сложности могут быть многостраничны, в то время как высказывание «*сложно рассчитать x* » - интуитивно понятно. Во-вторых, с методической точки зрения удобно увязывать понятия в систему и вводить их последовательно в соответствии со структурой курса. При проведении контроля от студента требуется прежде всего понимание сути тех или иных понятий и **умение оную суть внятно изложить.**



Общие сведения

Задачи КЗИ

Обеспечение конфиденциальности:

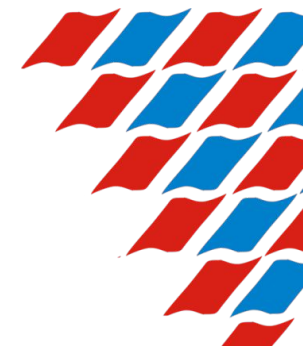
- Соккрытие содержания информации (ЗИ от НСД) - **шифрование**
- Скрытная передача информации (тайнопись) – **стеганография**

Обеспечение целостности:

- Защита от намеренной подмены (аутентификация сообщений) – **IMITOVCTABKИ, электронные подписи**
- Удостоверение авторства – **электронные подписи**
- Аутентификация пользователей – **серверы ключей, инфраструктуры открытых ключей**
- Удостоверение времени подписания документа, защита от подмены данных самим автором – **системы распределенного реестра**

Вспомогательные задачи:

- Вычисление псевдослучайного кода малой длины (дайджеста) – **хеш-функции**
- Вычисление псевдослучайного кода большой длины – **генераторы ПСП**



Общие сведения

«Большинство элементов системы безопасности напоминают стены и заборы тем, что не пропускают внутрь никого. Криптография же выполняет роль замка: она должна отличать хороший доступ от плохого»

«Система безопасности надежна настолько, насколько надежно ее самое слабое звено»

«Назначение криптографических протоколов состоит в минимизации объема доверия между участниками, необходимого для их взаимодействия»

Нильс Фергюссон, Брюс Шнайер «Практическая криптография»

Общие сведения

Защищаемая информация может представлять собой:

- Текст из символов естественного языка – **классическая криптография**
- Аналоговый сигнал – **скремблирование**
- Последовательность данных в двоичном коде – **современная криптография**



Общие сведения

В криптографии часто применяются **односторонние (необратимые) функции** и **функции с секретом**.

Функция $y = f(x)$ является односторонней, если не существует полиномиального способа вычислить x на основе известного y .

Коллизия односторонней функции – ситуация, когда два разных x дают в результате один и тот же y .

Функция $y = f(x_1, x_2, \dots, x_n)$ является односторонней для x_i , если не существует полиномиального способа вычислить x_i на основе известных y и всех остальных x .

Функция $y = f(k_1, x)$, где k_1 вычислено с помощью некоторой односторонней функции $k_1 = f_0(k_2)$, является функцией с секретом (функцией с ловушкой), если нет полиномиального способа вычислить x на основе известных y и k_1 , но существует полиномиальный способ вычислить x на основе известных y и k_2 . **Секретом** в данном случае называется значение k_2 .

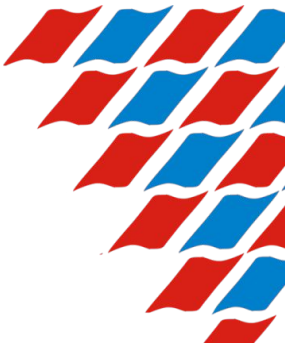


Общие сведения

Криптографическая хеш-функция

- **Необратимая** функция $y=f(x)$, где x – двоичный код произвольной длины, y – псевдослучайный двоичный код строго заданной длины (**дайджест сообщения**), такая, что...
- ...для любого заданного аргумента вычислительно невозможно подобрать другой, дающий то же значение (т.е. вычислительно невозможно получить коллизию хеш-функции)
- **Лавинный эффект**: при незначительном изменении x , y меняется радикально

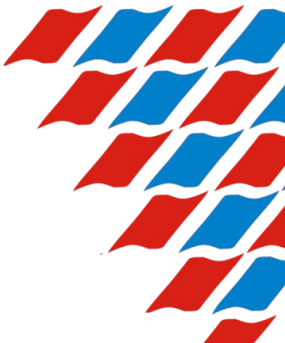
```
SHA3-256("The quick brown fox jumps over the lazy dog")=  
69070dda01975c8c120c3aada1b282394e7f032fa9cf32f4cb2259a0897dfc04  
SHA3-256("The quick brown fox jumps over the lazy dog.")=  
a80f839cd4f83f6c3dafc87feae470045e4eb0d366397d5c6ce34ba1739f734d
```
- Пример применения: проверка паролей, не требующая их хранения в памяти
 - **Функция формирования ключа** (Key derivation function, KDF) - хеш-функция, вычислительная сложность которой искусственно завышена, чтобы усложнить перебор паролей



Общие сведения

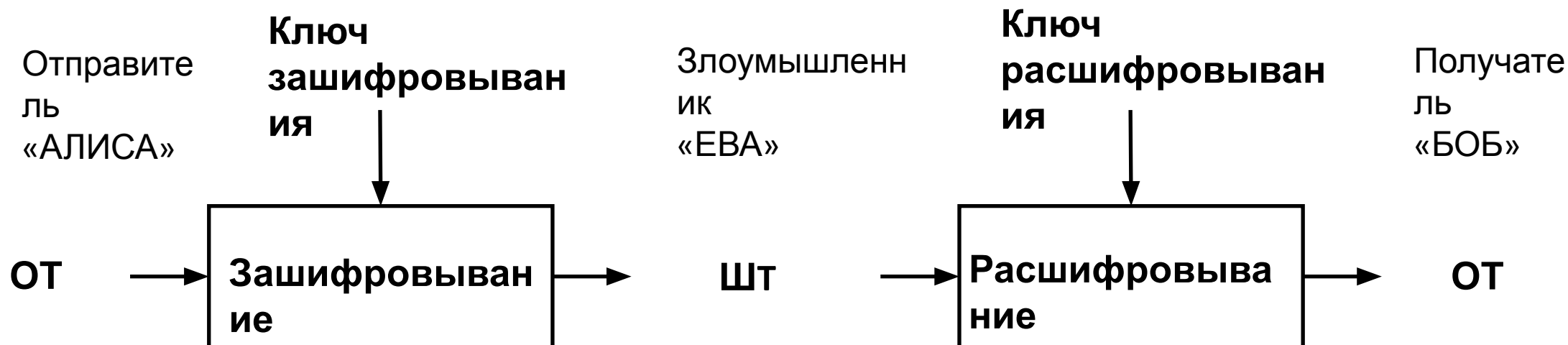
Криптографический генератор псевдослучайных последовательностей

- **Необратимая** функция $y=f(x)$, где x – двоичный код заданной длины, y – псевдослучайный двоичный код произвольной длины
- Псевдослучайная последовательность (ПСП) должна быть **непредсказуема вправо и влево** – должно быть невозможно вычислить на основе отдельного фрагмента ПСП остальные ее части



Общие сведения

Шифрование

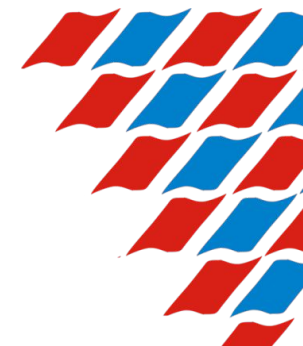


Цель – сделать сообщение **нечитаемым** для посторонних

Симметричное шифрование – ключи зашифровывания и расшифровывания совпадают

Асимметричное шифрование – ключи различны

Здесь и далее:
ОТ – открытый
текст
ШТ - шифротекст



Общие сведения

Шифрование

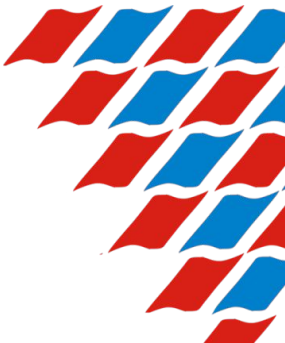
Симметричное

- Данные как двоичный код
- В основе – простые операции
- Сложное описание алгоритмов
- Можно придумать бесконечное множество алгоритмов
- Требуется мало ресурсов

Асимметричное

- Данные как целые числа
- В основе – сложный математический аппарат
- Простое описание алгоритмов
- В настоящее время известно лишь три базовых алгоритма с разными версиями
- Требуется много ресурсов

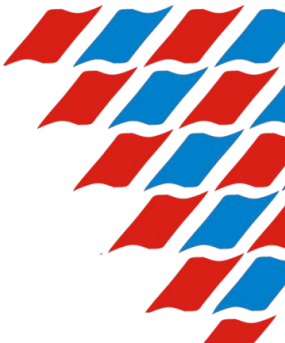
Хеш-функции обычно «тяжелее» симметричных шифров в разы и «легче» асимметричных на порядки



Общие сведения

Асимметричная криптосистема

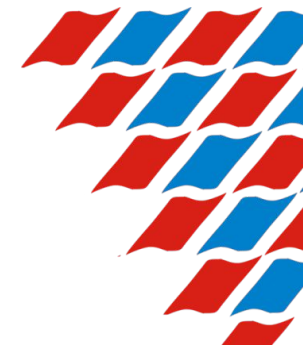
- Два ключа – **открытый** (ОК) и **закрытый** (ЗК)
- Вычислены на основе общей секретной информации, либо ОК на основе ЗК
- Нельзя вычислить ЗК на основе ОК
- ОК публикуется, ЗК хранится в тайне
- Если зашифровано на ОК, расшифровать можно на ЗК
 - Зашифровать может любой, расшифровать - только владелец ЗК
 - Используется для ЗИ НСД - **асимметричное шифрование**



Общие сведения

Асимметричные криптосистемы и электронные подписи

- Если зашифровано на ЗК, расшифровать можно на ОК
 - Зашифровать может только владелец ЗК, расшифровать - любой
 - Используется для удостоверения авторства - **электронная подпись (ЭП)**
 - Есть и другие способы построения электронной подписи ->
- Функция постановки электронной подписи
$$\text{ЭП} = f_{\text{sign}}(\text{ОТ}, \text{ЗК})$$
- Функция проверки электронной подписи
$$v = f_{\text{verify}}(\text{ОТ}, \text{ОК}, \text{ЭП})$$
 где v – логическая переменная; $v = \text{true} \Leftrightarrow \text{ОК}$ соответствует ЗК
- Для экономии вычислительных ресурсов электронные подписи как правило ставятся не на сам подписываемый файл, а на его хеш-функцию



Общие сведения

Имитовставка

Хэш-функция с ключом (имитовставка, код аутентификации сообщения, Message Authentication Code, MAC) – **необратимая** функция $y=f(x,k)$, где x – двоичный код произвольной длины, k – секретный ключ, y – псевдослучайный двоичный код заданной длины

- Используется, чтобы удостовериться, что сообщение дошло Бобу в том виде, в котором было отправлено Алисой

Стеганография

- Цель – сделать сообщение **незаметным** для посторонних
- Сообщение интегрируется в контейнер – массив данных, в котором оно будет незаметно (напр. изображение, аудиофайл, поток видеоданных и т.д.)
- **Пример.** В черно-белом изображении формата .bmp каждый пиксель кодируется одним байтом. Изменение значений последнего бита каждого байта не влияет на внешний вид изображения. Следовательно защищаемую информацию можно записывать в последние биты каждого байта изображения

Стеганография рассматривается в рамках курсов «Программно-аппаратные средства ЗИ» и «Теория информационной безопасности»



Общие сведения

Криптоанализ

- **Взлом шифра** – расшифровка шифротекста без знания ключа
 - Взлом хеш-функции или электронной подписи – нахождение коллизии
- **Атака на алгоритм** – попытка взлома
- Две стороны криптоанализа:
 - «Занятие злоумышленников»
 - Проверка на **криптостойкость** существующих алгоритмов
- Идеальный шифр можно взломать только полным перебором возможных значений ключа
 - Идеальную хеш-функцию/подпись – случайным перебором аргументов
 - Безопасная длина ключа - от 128(80) бит, безопасная длина хеш-функции – от 256(160)
- Когда говорят «алгоритм взломан» – часто подразумевается взлом «в теории»: способ нахождения ключа (коллизии), более быстрый, чем перебор
 - На практике алгоритм может оставаться криптостойким
 - Пример: «взлом» ГОСТ28147-89 в 2012 году - требуется 2^{224} операций зашифровывания при наличии у злоумышленника 2^{32} пар ОТ-ШТ

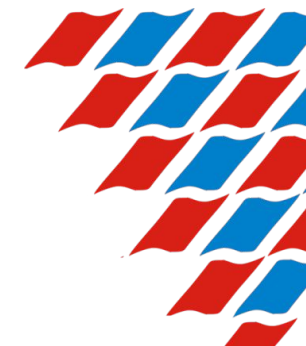
найден



Общие сведения

Правило Керкгоффса

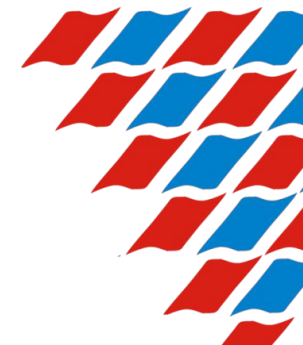
- В общем виде: «хороший криптографический алгоритм нельзя взломать, **зная, что был применен именно этот алгоритм, но не зная ключа**»
 - Для шифрования – нельзя **расшифровать шифротекст**, зная <...>
 - Для стеганографии – нельзя отличить пустой контейнер от контейнера, содержащего стеганограмму, зная <...>
- Практические следствия:
 - Популярность алгоритма сама себя усиливает
 - Применяются почти исключительно свободно распространяемые алгоритмы
- Противоположный подход: «Безопасность через неясность» [Security through obscurity]
 - Подход может создавать дополнительный уровень безопасности, но при этом секретный алгоритм должен быть безопасен сам по себе.



Общие сведения

Основные атаки на шифры

- Cipher-text-only – у Евы есть только шифротекст и знание, какой алгоритм применен
- Known-plaintext – у Евы есть набор пар открытый текст / шифротекст
 - Функция зашифровывания должна быть односторонней как относительно шифруемого текста так и относительно ключа
- Chosen plaintext / ciphertext – Ева может узнать, какой шифротекст / открытый текст соответствует заданному открытому тексту / шифротексту
- Meet in the middle – у Евы есть множество предполагаемых ключей и множество зашифрованных сообщений; при прослушивании канала связи она ожидает, когда появится сообщение, которое есть в множестве; по нему можно определить ключ
- Man in the middle – Ева подключена к каналу связи таким образом, что может управлять трафиком между Алисой и Бобом
- Related key – у Евы есть множество шифротекстов, зашифрованных разными ключами и знание, что эти ключи связаны между собой



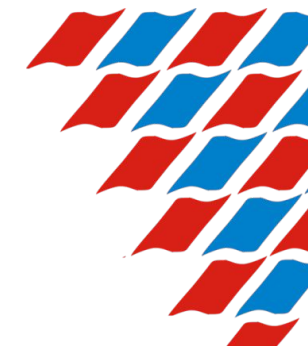
Общие сведения

Основные атаки на хеш-функции

- Collision search – поиск другого аргумента, дающего то же значение, что и заданный
- Birthday attack – поиск пары аргументов, дающих одно и то же значение
 - Хеш-функция, устойчивая к атаке дней рождения называется **сильной**

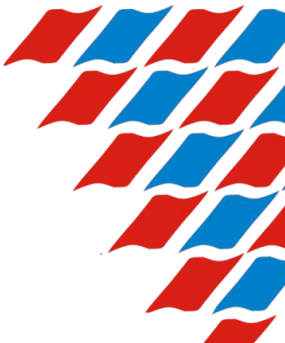
Виды атак с технической точки зрения

- Атаки на любую криптосистему могут быть **оперативными** (злоумышленник взаимодействует с криптосистемой) и **автономными** (злоумышленник работает на своем компьютере без связи с системой)
- Особая разновидность - **атаки с использованием побочных каналов**
 - Злоумышленник анализирует косвенную информацию о работе криптосистемы – побочное излучение, энергопотребление, время выполнения команд (**тайминг-атаки**) и т.п.
 - Актуальны для специализированного аппаратного обеспечения (смарт-карт)



Содержание лекции

- Структура курса
- Общие сведения о криптографии
- **Исторический обзор**
 - **Классическая криптография**
 - **Скремблирование**
 - **Современная криптография**
 - **Персоналии**
 - **Художественная литература**



Исторический обзор

Классическая криптография

Перестановочные шифры

- V в. до н. э. «Считала Лисандра»
- Ключ – порядок перестановки

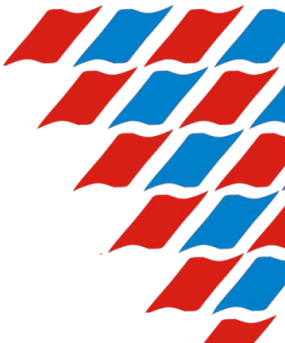
Подстановочные шифры

- I в. до н. э. «Шифр Цезаря»
- Ключ – таблица замен
- Способ взлома – частотный анализ символов

В XIX веке начали развиваться шифровальные машины, которые могли использовать комбинации подстановок и/или перестановок

С середины XX века классическая криптография утратила свое значение

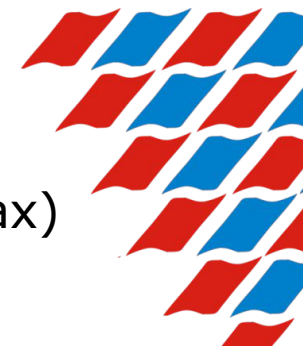
1999 – шифр Solitair (Pontifex)



Скремблирование

Пример: защита телефонных разговоров от прослушивания

- Для речевого сигнала значимый диапазон 500-3000 Гц
- За пределами звук есть, но на разборчивость не влияет
- Фонемы – отдельные произносимые звуки
 - Гласные – поток воздуха через голосовые связки, ~100 мс
 - Взрывные – полное перекрытие потока губами, ~5 мс (п, к, т и т.д.)
 - Фрикативные – частичное перекрытие, 20-50 мс (ф, с, ш и т. д.)
- В русском языке ~40 фонем
- Скремблирование защищает от злоумышленников, не обладающих специальными техническими средствами
- 2 типа преобразований сигнала:
 - Частотные преобразования - модифицируется спектр сигнала
 - Временные преобразования - обработка сигнала на временных отрезках (кадрах)



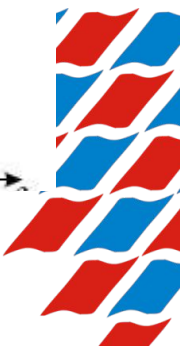
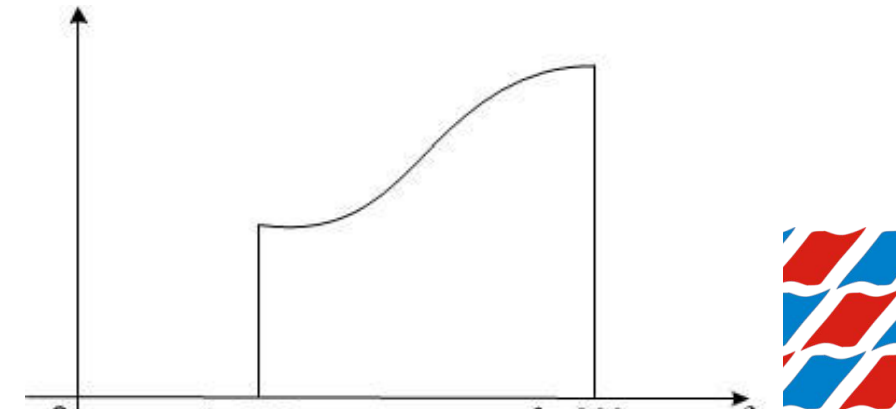
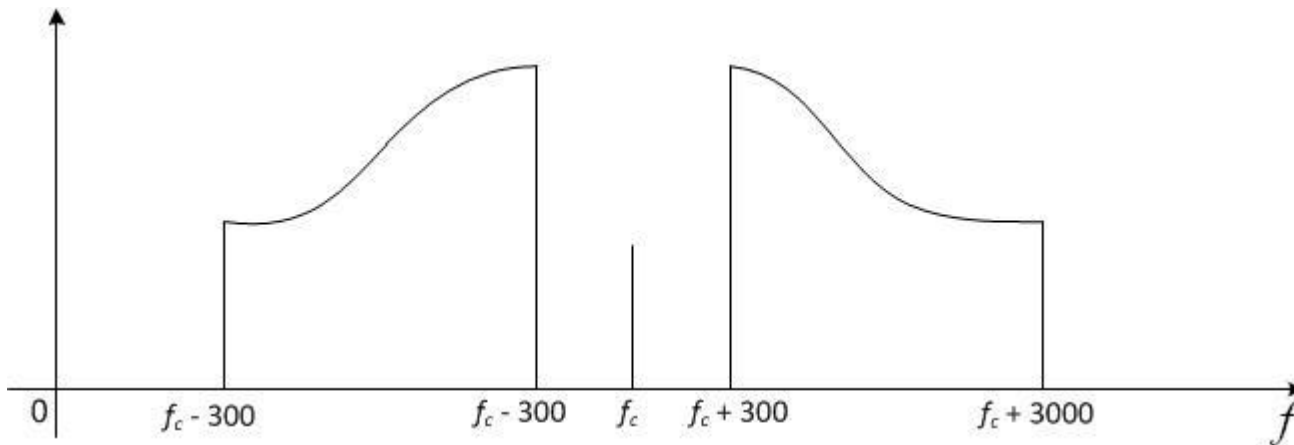
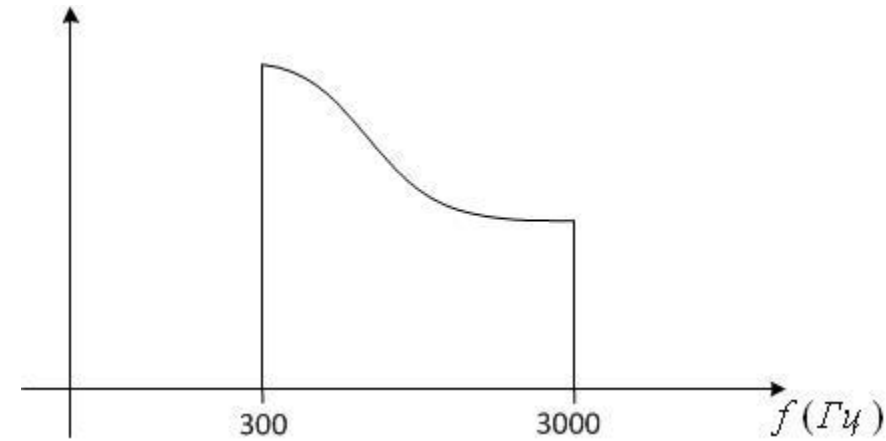
Скремблирование

Инверсия спектра

Спектр сигнала отзеркаливается

Смеситель – отражает сигнал относительно
некоторой несущей частоты

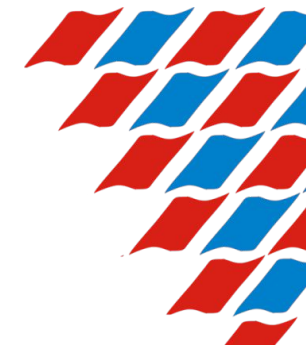
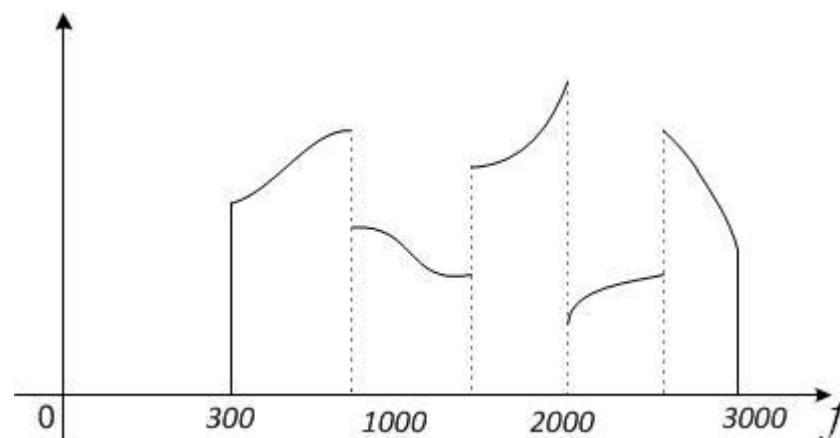
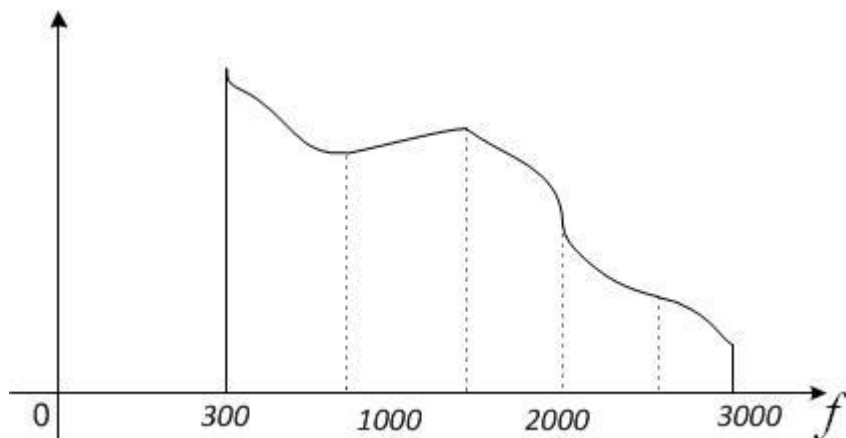
На смесителях с разными несущими строятся
аналоговые многоканальные линии



Скремблирование

Перестановка частот

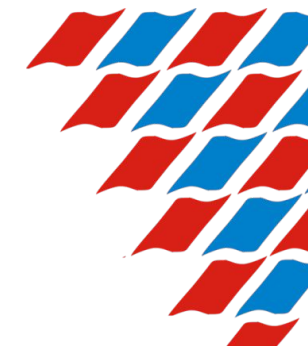
Диапазоны на спектре меняются местами
Часть диапазонов может инвертироваться



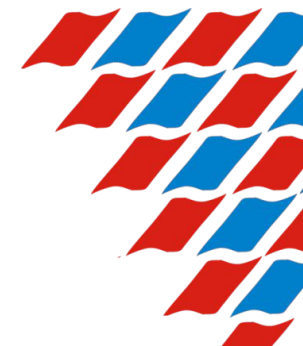
Скремблирование

Временные преобразования

- Кадр делится на сегменты
- Обычно кадр из 8-16 сегментов по 20-60 мс
- Меньшая длина сегмента – хуже качество
- Большая длина кадра – большая задержки
- Преобразования, аналогичные частотным:
 - инверсия кадра
 - перестановка сегментов



- 1917 - Шифр Вернама
- 1920е-30е - Гаммирование
- 1945 – Клод Шеннон «Теория связи в секретных системах»
- 1972-77 – Сеть Фейстеля, разработка алгоритма DES (56-битный ключ)
- 1990-е – Возросшая мощность компьютеров позволила взламывать DES полным перебором ключей
- 1997-2000 Конкурс AES
 - Цель – выбор алгоритма на замену DES в качестве стандартного
 - Длина ключа – 128, 192, 256 бит
 - Простота программной реализации, работа на 32-разрядных процессорах (DES заточен под аппаратную реализацию)
 - Победитель (RIJNDAEL) стал стандартом AES
 - Ряд не прошедших конкурс алгоритмов нашли свое применение (RC6, Twofish)

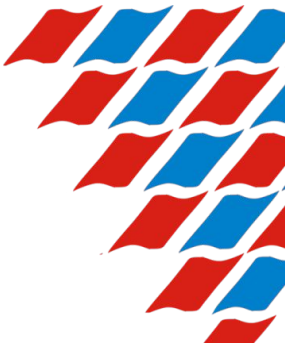


Асимметричная криптография

- 1970-е – Теоретические работы Диффи, Хеллмана, Меркла («задача об укладке рюкзака»)
- 1977 – Алгоритм RSA
- 1991 – DSA
- 1998 – DSS (DSA + SHA-1)
- 1999 - ECDSA

Хеш-функции

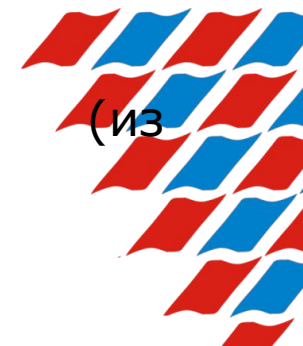
- 1990 MD4
- 1995 SHA-1
- 2002 SHA-2
- 2007-2012 Конкурс SHA-3.
Победитель – алгоритм Кессак
- 2013-2017 Взломы SHA-1.
Отказ от использования алгоритма



Современная криптография

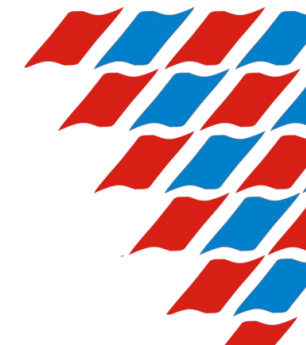
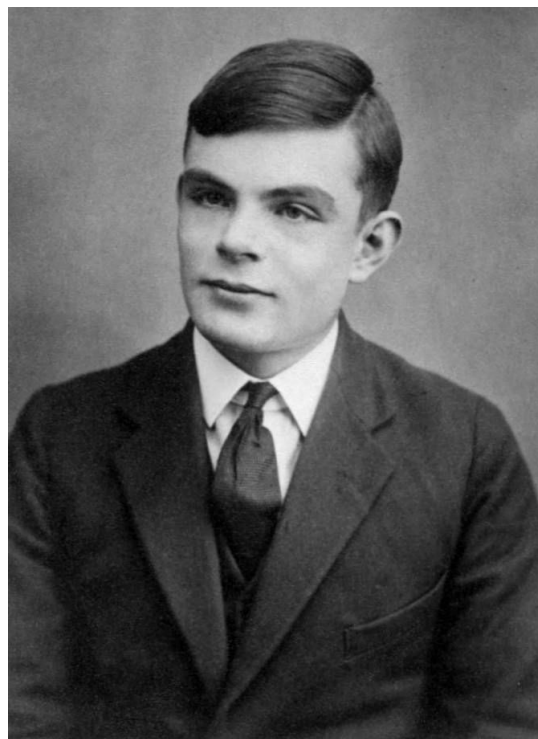
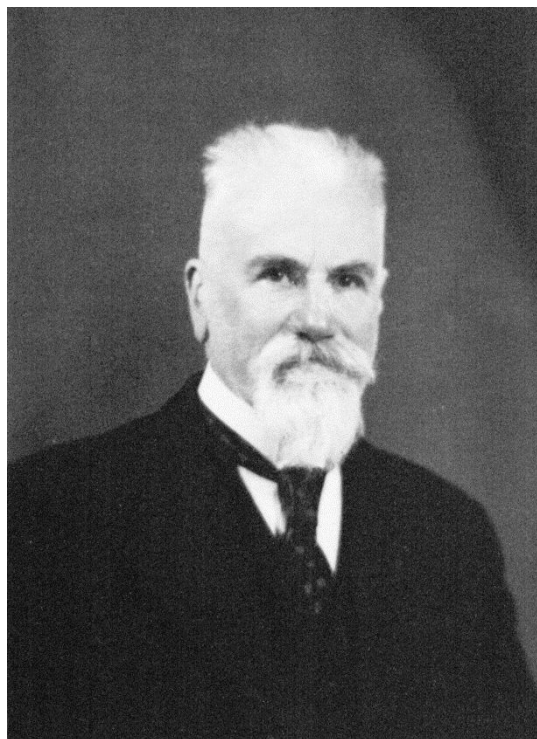
Криптография в СССР и России

- 1937 – К-37 «Кристалл» (классическое шифрование) и М-100 «Спектр» (гаммирование)
- 1989 – ГОСТ 28147-89 – симметричный алгоритм (возможно, разработан в 70-е)
- 1994 – ГОСТ Р 34.11-94 – хэш-функция
- 1994 - ГОСТ Р 34.10-94 – ЭЦП на дискретных логарифмах (для хэширования применяется ГОСТ Р 34.11-94)
- 2001 - ГОСТ Р 34.10-2001 – новый стандарт ЭЦП (по сути – версия ГОСТ Р 34.10-94 на эллиптических кривых)
- Новые стандарты разработаны ФСБ совместно с ОАО «ИнфоТекс»
 - 2012 - ГОСТ Р 34.11-2012 – новая хэш-функция «Стрибог»
 - 2012 - ГОСТ Р 34.10-2012 – стандарт ЭЦП (по сути ГОСТ Р 34.10-2001, но для хэширования применяется Стрибог)
 - 2015 (2018) – ГОСТ Р 34.12-2015 (-2018) – симметричные алгоритмы «Магма» (старого ГОСТа) и «Кузнечик»



Персоналии

Огюст Керкгоффс (1835-1903), Алан Тьюринг (1912-1954), Клод Шеннон (1916-2001)



Персоналии

Хорст Фейстель (1915-1990)

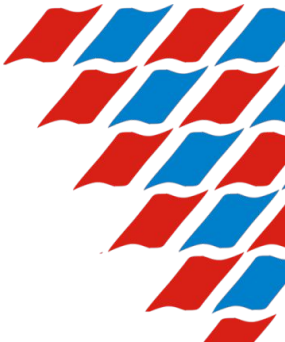
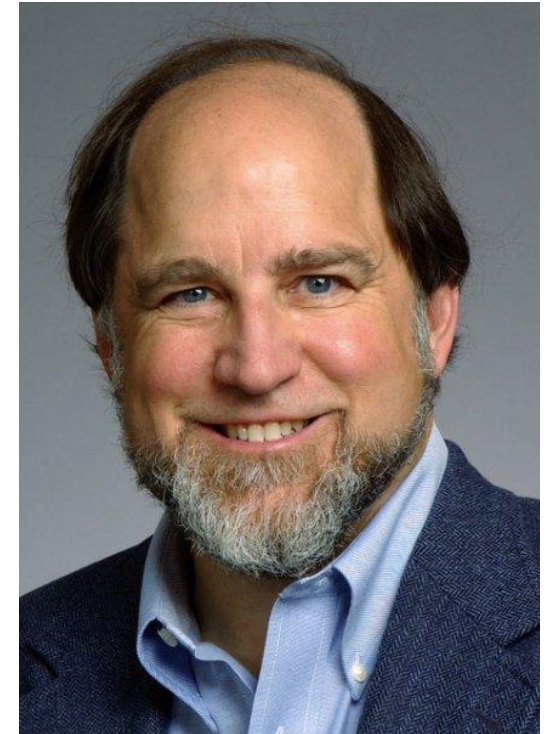
- Первый крупный неправительственный автор шифров
- По сути создатель современного подхода к построению симметричных шифров
- Автор шифра Lucifer, позднее переделанного в DES



Персоналии

Рональд Райвест (род. 1947)

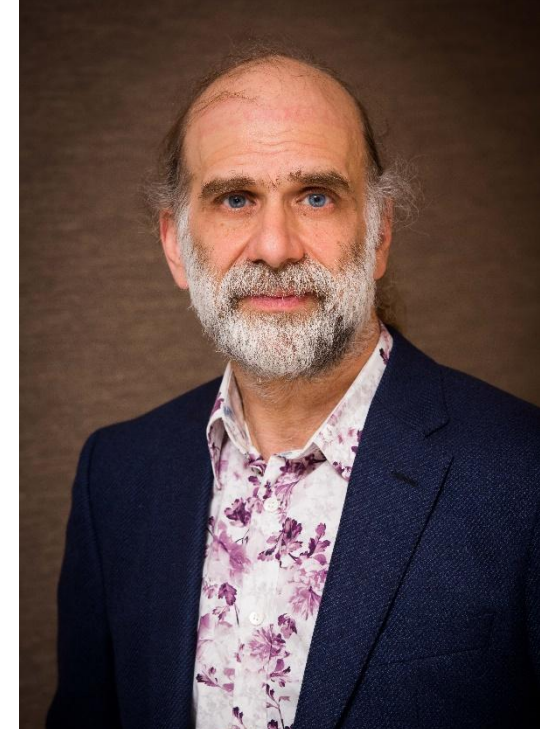
- Асимметричный алгоритм RSA (1977, совместно с А. Шамиром и Л. Эйдельманом)
- Блочные симметричные шифры: RC2 (1987), RC5 (1994), RC6 (1998)
- Поточный шифр RC4 (1987)
- Хеш-функции: MD2 (1989), MD4 (1990), MD5 (1991), MD6 (2008)



Персоналии

Брюс Шнайер (род. 1963)

- Блочные симметричные шифры: Blowfish (1993), Twofish (1998), Threefish (2008)
- Хеш-функция Skein (2008)
- Генератор псевдослучайных чисел с добавлением истинной случайности Fortuna (2003)
- Классический шифр Solitaire (1999)
- Блог <https://www.schneier.com/>
- Книги:
 - Прикладная криптография (1994)
 - Практическая криптография (2003, совместно с Н. Фергюссоном)



Художественная литература

- 1843 Эдгар По «Золотой Жук»
- 1864 Жюль Верн «Путешествие к центру Земли»
- 1905 Артур Конан Дойль «Пляшущие человечки»
- 1999 Нил Стивенсон «Криптономикон»
- 2010 Ханну Райанниэми «Квантовый вор»